UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/788,677	02/27/2004	Michael D. Smith	418268004US	3591

45979 7590 11/14/2011

PERKINS COIE LLP/MSFT
P. O. BOX 1247
SEATTLE, WA 98111-1247

EXAMINER	
EVANS, KIMBERLY L	
ART UNIT	PAPER NUMBER
3629	

NOTIFICATION DATE	DELIVERY MODE
11/14/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentprocurement@perkinscoie.com

Office Action Summary	Application No.	Applicant(s)	
	10/788,677	SMITH ET AL.	
	Examiner	Art Unit	
	KIMBERLY EVANS	3629	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,2,5,7-11,22,23 and 25-29* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,2,5,7-11,22,23 and 25-29* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

Response to Remarks

1. This action is in reply to the remarks filed on August 1, 2011.

2. Claims 1, 2, 5, 7-11, 22, 23, and 25-29 are currently pending and have been examined. The Examiner has carefully reviewed the Applicant's response and has determined that the rejection stands and is resubmitted below addressing the claims as modified by said amendments.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

(a) Determining the scope and contents of the prior art.

(b) Ascertaining the differences between the prior art and the claims at issue.

(c) Resolving the level of ordinary skill in the pertinent art.

(d) Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 1, 2, 5, 7-11, 22, 23, and 25-29 are rejected under 35 USC 103(a) as being unpatentable over Medvinsky et al., US Patent Application Publication No US 2003/0093694 A1, in view of Zhang et al., US Patent Application Publication No US 2005/0076220 A1.

6. With respect to Claims 1, 11, 22, and 25,

Medvinsky discloses the following limitations,

- *acquiring by the processor, a block of tickets at a time from a ticketing entity, the block of tickets including at least one ticket having a value specified by a sender of a message*
- *receiving an electronic message having a ticket issued by a ticketing entity, the ticket having a value that is specified by a sender*

(see at least Figure 1, paragraph 16: "...Note that the user may have previously obtained a caching server ticket from the KDC. A ticket is an authentication token and it may include the client, a server name, a session key, etc. The ticket further contains authorization data indicating subscribed services, user payment method, etc. This ticket and the session rights object are thereafter presented to the caching server which

compares user selection and/or content access rules in the session rights object with authorization data from the ticket..."; paragraph 28: "...IPRM system 200 comprises a content provider 202, consumer 216, Internet 214, a provisioning center 206, a central server 205 that contains both a database 208 and a search engine 210, caching servers 212, 213 and 215 all of which function in a similar manner to those of the corresponding components in FIG. 1. In addition, IPRM system 200 comprises a KDC (key distribution center) 204 containing an AS (authentication server) 207 for issuing a TGT (ticket granting ticket) to consumer 216, a TGS (ticket granting server) 209 for providing server tickets to access particular servers, a provisioning server 220, and a billing center 211..."; paragraph 36: "...In order to authenticate a message with a ticket (e.g. ESBroker Key Request message), a client would include in this message both a ticket and a checksum value for the session key in the ticket...")

- *each ticket of the block including a code from a sequence of codes generated from a start code using a one-way function*; (see at least paragraph 95: "...Each packet may be encoded..."; paragraph 97: "...These parameters are: EK--RTP encryption key; an Initialization Vector (IV), which is derived from the RTP packet header using a one-way function. It should be observed that because each RTP packet header contains a different sequence number or timestamp, it results in a unique IV per packet....")

- *adding the acquired ticket to the message and forwarding the message with the added ticket to a recipient,* (see at least paragraph 36: "…In order to authenticate a message with a ticket (e.g. ESBroker Key Request message), a client would include in this message both a ticket and a checksum value for the session key in the ticket….")
- *and wherein a mail server is provided with an end code of the sequence of codes and determines whether a ticket of the message includes a code from which the end code can be derived.*
- *wherein the ticketing entity receives an end code of a sequence of codes and determines whether the ticket includes a code from which the end code can be derived and charges the sender for a value of the ticket* (see at least paragraphs 88-117:"...Streaming and Non Streaming Content..."...RTP (real time protocol)/RTCP (real time control protocol), RTSP (real time streaming protocol). Non-streaming transfer of content between servers: Streaming Description: RTSP with SDP (session description protocol). Other Non-Streaming Content: HTTP (provisioning, content publishing to the directory); Custom protocols over either TCP (transport control protocol) or UDP (user datagram protocol) (content usage reporting). Streaming Content. In standards-based systems, the streaming content is typically delivered using the RTP. There are additional proprietary streaming protocols such as Real and Microsoft's Windows Media that can also be secured with this IPRM system..." and

paragraphs 90-117 "... RTP Security Services, RTP, RTCP, and RTSP Packet Encoding, RTP, RTCP, and RTSP Decoding, Cryptographic Mechanisms, Secure session identifiers, Packet sequence numbers, Message Authentication Code (MAC) with respect to message integrity and number sequencing, session number verification for application messages, RTSP Encoding and RTSP Message Decoding..."; paragraphs 108-113: ...sequence number verification methods for application messages sent over TCP and UDP).

Medvinsky discloses all of the above limitations, Medvinsky does not distinctly disclose the following limitations, but Zhang however, as shown discloses,

- *presenting the electronic message to a recipient*
- *wherein the message is an electronic mail message* (see at least Abstract: "...For every email sent from a sender to a recipient using the system built upon the present invention..."
- *when the recipient indicates to redeem the ticket, submitting by the processor the ticket to the ticketing entity for redemption*, (see at least Abstract: "...the sender's allotment of anti-spam points would be deducted by a fixed or varied number, depending on the specific implementation of the particular embodiment of the present invention..."; paragraph 20: "...The system comprises the Email Chief for issuing and verifying the fingerprint keys, and issuing and deducting the points...")

- *wherein upon receiving the message, the recipient can conditionally, redeem the value of the ticket from the ticketing entity* (see at least at least paragraph 22: "...a method of acknowledging delivery of the email and deducting the anti-spam points is provided. The method comprises the steps of: 1) the Email Chief checking the file to verify the sender is registered and the provided fingerprint key is correct, 2) acknowledging the recipient's email server or email client to deliver the email, and 3) deducting the appropriate anti-spam points from the sender..."; paragraph 67: "...function of holding the email and communicating with the Email Chief can be done by the recipient's email client....")
- *when the recipient does not indicate to redeem the ticket, suppressing the redeeming of the ticket so that the recipient can conditionally redeem tickets* (see at least paragraph 21: "...the Email Chief asking the recipient's server to hold the email, and 4) the Email Chief sending a message to the sender requesting the sender to register...."; paragraph 37: "...A ticket may have other information as well, including a validity period (start time and expiration time), various flags, client authorization data, etc....")
- *wherein a sender's account and a recipient's account are maintained by the same entity* (see at least paragraph 78: "...The system comprises the Email Chief for issuing and verifying the fingerprint keys, and issuing and deducting the points...")

- *wherein a sender's account and a recipient's account are maintained by different entities* (see Figure 1, paragraph 108: "...The system includes a sender's computer S, a recipient's computer R, the sender's SMTP email server MO, the recipient's email server MI, and the Email Chief C for registration/authentication purposes. The present invention can be deployed at the recipient's email server MI or at the recipient's email client software R, and at the Email Chief C. The Email Chief C has the function for registration, authentication, and maintenance of database...")

Upon further search of the primary reference, Medvinsky teaches at least a KEY_REQ message containing a MAC (message authentication code) of the message; and that the KDC 204 service key also used to authenticate the TGT with a "keyed hash" (paragraph 42). Medvinsky further discloses various cryptographic mechanisms to include but not limited to packet coding and decoding, and sequence number verification methods for application messages sent over TCP and UDP (paragraphs 108-117). Zhang teaches the "...Email Chief is the encoded string containing the sender's email address and the fingerprint key paragraph 33) and that the Email Chief matches the fingerprint key with the one in the record for a given address for message authentication. Both Medvinsky and Zhang teach various mechanisms used for authentication (with respect to transaction integrity and secrecy) of electronic messages.

These mechanisms are old and well known in the cryptographic art. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of Medvinsky with the system of Zhang because it would provide an efficient means for differentiating spammers from non-spammers via cryptographic mechanisms for authentication, to include but not limited to registering and verifying the sender's fingerprint key, and deducting sender's anti-spam points for delivery of electronic message(s) to the recipient.

7. With respect to Claim 2,

Medvinsky and Zhang disclose all of the above limitations, Medvinsky further discloses,

- *the acquired ticket includes a sender authenticating code so that a mail server that receives the message can authenticate the sender of the message.* (see at least paragraph 42: "...the private portion of the TGT is encrypted with KDC 204's service key known only to KDC 204. The same KDC 204 service key is also used to authenticate the TGT with a keyed hash..."; paragraph 45: "...The ticket is also authenticated with a hash that is keyed with the same service key..."; paragraph 47: "...The KEY_REQ message contains a MAC (message authentication code) of the message...")

8. With respect to Claim 5,

Medvinsky and Zhang disclose all of the above limitations, Medvinsky further discloses,

- *wherein the tickets are added to messages in reverse order of generation of their codes.*(see at least paragraph 197: "...Note that the derivation order of the inbound and outbound keys at the client and server are reversed.....")

9. With respect to Claims 7, 27 and 29,

Medvinsky and Zhang disclose all of the above limitations, Zhang further discloses,

- *the recipient's mail system can validate the ticket with the ticketing entity before presenting the message to the recipient* (see at least paragraph 19: "...The method comprises verifying the sender's fingerprint key and deducting sender's anti-spam points before acknowledging the recipient's email server to deliver the email...")
- *validating that the ticket can be redeemed before presenting the ticket to the recipient*

  (see at least paragraph 22: "...a method of acknowledging delivery of the email and deducting the anti-spam points is provided. The method comprises the steps of: 1) the Email Chief checking the file to verify the sender is registered and the provided fingerprint key is correct, 2)

acknowledging the recipient's email server or email client to deliver the email, and 3) deducting the appropriate anti-spam points from the sender..."; paragraph 67: "...function of holding the email and communicating with the Email Chief can be done by the recipient's email client....")

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the concepts of tickets and the cryptographic tools of Medvinsky with the email messaging system of Zhang because it provides an efficient means for delivering legitimate electronic messages without spamming recipients.

10. With respect to Claim 8,

Medvinsky and Zhang disclose all of the above limitations, Zhang further discloses,

- *the recipient's mail system can automatically discard messages with ticket values below a threshold value set by the recipient.*(see at paragraph 41: "...If the recipient's threshold value is lower than the advertiser's threshold value, then the email will be delivered, and if not, the email will not be delivered. ...")

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the concepts of tickets and the cryptographic tools of Medvinsky with the email messaging system of Zhang because it provides an

efficient means for a recipient to set a threshold value for unsolicited messages according to his or her opportunity costs.

11. With respect to Claims 9, 23 and 28,

Medvinsky and Zhang disclose all of the above limitations, Zhang further discloses,

- *when the recipient redeems the ticket, an account of the sender is debited.*
- *wherein the redemption includes decreasing an account balance of the sender and increasing an account balance of the recipient*

(see at least Abstract: "...every email sent from a sender to a recipient using the system built upon the present invention, the sender's allotment of anti-spam points would be deducted by a fixed or varied number, depending on the specific implementation of the particular embodiment of the present invention ..."; paragraph 20: "...The system comprises the Email Chief for issuing and verifying the fingerprint keys, and issuing and deducting the points; claim 12 e) : "...and adding appropriate quantities and appropriate types of anti-spam points to recipient's record...")

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the concepts of tickets and the cryptographic tools of Medvinsky with the email messaging system of Zhang because the Email Chief provides an efficient means for issuing, deducting and tracking points for registered email senders.

12. With respect to Claims 10 and 26,

Medvinsky and Zhang disclose all of the above limitations, Zhang further discloses,

- *when the recipient redeems the ticket, an account of the sender is credited.*
- *wherein the entity that maintains the sender's account transfers the value to the entity that maintains the recipient's account.*

(see at least paragraph 20: "...The system makes available an online registration form, and when the sender completes the form, the system would issue a certain number of free (no charge) anti-spam points, hereinafter referred to as Pass Points..."; paragraph 54: "...the Email Chief C can send registration requests to email senders that are not in the current pool of registered users, can communicate with email senders, can issue a fingerprint key for each email address after a successful registration, can issue a certain amount of free Pass Points for the email address, and can replenish or infuse it with more Pass Points after a fixed or varied period of time. These free Pass Points will be deducted by a fixed or varied number each time the user sends out an email to the email servers adopting the present invention. These free Pass Points will be automatically replenished for the user after a fixed or varied period of time has elapsed..."; paragraph 63: "...if the Email Chief C can match the

fingerprint key with the one in the record for the given email address, and verifies that the limit on the number of Ad points offered to the recipients meets or exceeds the threshold value for charging paid Ad Points set by the recipient R, then B deduct from sender S' account the number of Ad points that matches R's threshold value, and credits them to R's account....")

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the concepts of tickets and the cryptographic tools of Medvinsky with the email messaging system of Zhang because the Email Chief provides an efficient means for issuing and/or tracking anti-spam points, and verifying fingerprint keys for registered email senders.

Response to Arguments

13. Applicant's arguments filed August 1, 2011 have been fully considered but are not persuasive. Examiner uses the primary reference Medvinsky to teach the concept of tickets. A ticket is used to securely pass to a server a session key along with the identity of the client for whom the ticket was issued. A ticket is tamperproof and can be safely stored by the clients, allowing servers to remain stateless (a server can re-learn the session key each time that the client passes it the ticket). Thus, the concept of tickets improves scalability of servers in terms of the number of clients that they can support..." (paragraph 6). As noted above and in Examiner's Action, Medvinsky teaches that a ticket

contains authorization data to include but not limited to user payment method, and subscribed services and an authentication token which may include the client, a server name, a session key etc (paragraph 16). Medvinsky further teaches "...IPRM system 200 comprises a KDC (key distribution center) 204 containing an AS (authentication server) 207 for issuing a TGT (ticket granting ticket) to consumer 216, a TGS (ticket granting server) 209 for providing server tickets to access particular servers, a provisioning server 220, and a billing center 211. KDC 204, billing center 211, provisioning center 206 and central server 205 are all located within a central unit 218 for facilitating provision of services within IPRM system 2000 (paragraph 28). Medvinsky discloses that the private portion of the TGT is encrypted with KDC 204's service key known only to KDC 204. The same KDC 204 service key is also used to authenticate the TGT with a "keyed hash" (paragraph 42), and that "...the KEY_REQ message contains a MAC (message authentication code) of the message, DOI (domain of interpretation) object and a time stamp in addition to the caching server ticket..." (paragraph 47). Medvinsky discloses two basic categories of content that are protected, streaming and non-streaming and the various protocols used (paragraphs 88-117) to include in standards-based systems, the streaming content is typically delivered using the RTP. Medvinsky further teaches additional proprietary streaming protocols such as Real and Microsoft's Windows Media that can also be secured with the IPRM system..." (paragraph 90). Examiner relies upon the

secondary reference, Zhang to teach (conditional) redemption of (anti-spam) points (i.e. value of the ticket) depending on the specific implementation via an email management system, the Email Chief. Zhang's email management system includes a sender's computer S, a recipient's computer R, the sender's SMTP email server MO, the recipient's email server MI, and the Email Chief C for registration, authentication, and maintenance of the database (paragraph 108). The Email Chief is the encoded string containing the sender's email address and the fingerprint key (paragraph 33). The Email chief issues and verifies the fingerprint keys, and sender's anti-spam points prior to delivery of the email, or holds the email if the information is incorrect (paragraphs 20 and 21). Anti-span points are purchased from the Email Chief operator. Zhang further discloses the anti-spam points are categorized into four types: Pass points, Dom points, Safe points, and Ad points. The Pass points and Dom points are issued free of charge, while the Safe points and Ad points are required to be purchased (paragraph 110). By way of the Email Chief, anti-spam points are identified, issued, compared and redeemed and attached to a sender's email in addition to the fingerprint key which authenticates and identifies the sender. Examiner has pointed out particular references contained in the prior art of record within the body of the office action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply.

Applicant should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

14. With respect to applicant's arguments on page 7 of the remarks regarding claim 1, "...upon receiving the message, the recipient can conditionally redeem the value of the ticket from the ticketing entity, and wherein a mail server is provided with an end code of the sequence of codes and determines whether a ticket of the message includes a code from which the end code can be derived... The Office Action concedes that Medvinsky does not disclose anything remotely similar to these features, but points to Zhang as overcoming this deficiency. ... the Office Action does not indicate where in Zhang the features "conditionally redeem the value of the ticket from the ticketing entity" or "including a code from which the end code can be derived" are taught or suggested...". Examiner is not persuaded that neither the primary reference, Medvinsky nor Zhang teaches "...a mail server provided with an end code of a sequence of codes and determines whether a ticket of the message includes a code from which the end code can be derived...". Upon further examination of the primary reference, it is pointed out in this Office Action that Medvinsky discloses various cryptographic mechanisms (paragraph 92) to include but not limited to the IPRM agents in conjunction with KDC 204 and that the KDC provides key distribution to network

components using a blend of symmetric and asymmetric algorithms which may be provided in secure cryptographic hardware. Medvinsky discloses two basic categories of content that are protected, streaming and non-streaming, and the various protocols used (paragraphs 88-117) including RTP Cryptographic mechanisms and sequence number verification methods for application messages sent over TCP and UDP (paragraphs 108-113). While Zhang discloses a fingerprint key consisting of a string chosen by the email sender during registration. The fingerprint key is typed in the body of the email as if it is part of the email message and the Email Chief matches the fingerprint key with the one in the record for a given address for message authentication.). The Email chief issues and verifies the fingerprint keys, and sender's anti-spam points prior to delivery of the email, or holds the email if the information is incorrect (paragraphs 20 and 21). Zhang further teaches a digital signature certificate generated by cryptographic software for authentication purposes (paragraph 66). Both Medvinsky and Zhang teach various cryptographic mechanisms used for authentication (with respect to transaction integrity and secrecy) of electronic messages. Moreover, the mechanisms used for authentication (with respect to transaction integrity and secrecy) in the cryptographic art are old and well known. MAC is like hash code for a sequence of bytes. MAC uses a secret key to generate the hash code, and is generally used to check the integrity or validity of information based on a secret key. Crytography security-analysis measures processes

(algorithm(s) sets), and provides protection against modification of the hash via encryption with a secret key. In this case, both the sender and receiver must have it for successful access, transmittal and retrieval. Other cryptographic subsystems may be added to messages or may follow as sub-protocols, for example an electronic payment system that follows a successful transaction. Medvinsky and Zhang utilize various cryptographic mechanisms for authentication to include sequence number verification methods (Medvinsky), while Zang further discloses an Email chief for issuing, and verification of fingerprint keys, and sender anti-spam points prior to delivery of an email. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the concepts of tickets and the cryptographic tools of Medvinsky with the email management system of Zhang because it would provide an efficient means for authenticating electronic messages, and email marketing, including but not limited to advertisers capable of buying Ad Points and setting thresholds for sending emails, while enabling email recipients to set personal threshold values for receiving emails from senders (Zhang paragraphs 40-42), hence differentiating spammers from non-spammers and deducting sender's anti-spam points. Applicant always has the opportunity to amend the claims during prosecution and broad interpretation by the examiner reduces the possibility that the claim, once issued, will be interpreted more broadly than is justified. *In re* Prater, 162 USPQ 541,550-51 (CCPA 1969). In view of the

above, the Examiner contends that all limitations as recited in the claims have been addressed in this Office Action. For the above reasons, Examiner believes that the rejections in this Office Action are proper. Detailed explanations are given in the preceding sections of the present Office Action.

Conclusion

15. **THIS ACTION IS MADE FINAL.** See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37CFR 1.136(a).

16. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period fro reply expire later than SIX MONTHS from the date of this final action.

17. Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **Kimberly L. Evans** whose telephone number is

571.270.3929. The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **Jami Plucinski** can be reached at **571.272.6811.**

18. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair <http://pair-direct.uspto.gov >. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free). Any response to this action should be mailed to: **Commissioner of Patents and Trademarks**, P.O. Box 1450, Alexandria, VA 22313-1450 or faxed to **571-273-8300**. Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**: Randolph Building 401 Dulany Street, Alexandria, VA 22314.

/KIMBERLY EVANS/
Examiner, Art Unit 3629

/Jamisue A Plucinski/

Supervisory Patent Examiner, Art Unit 3629